STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

INFORMATION WARFARE AND ARMY GUARD READINESS

BY

LIEUTENANT COLONEL RICKY W. STREIGHT
United States Army National Guard

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20000526 073

DTIC QUALITY INSPECTED 3

USAWC STRATEGY RESEARCH PROJECT

Information Warfare and Army Guard Readiness

by

Lieutenant Colonel Ricky W. Streight, Ph.D.
Oklahoma Army National Guard

Colonel Robert E. Wright
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: Ricky W. Streight

TITLE: Information Warfare and Army Guard Readiness

FORMAT: Strategy Research Project

DATE: 03 March 2000 PAGES: 24 CLASSIFICATION: Unclassified

Information warfare and its several variants and/or components such as cyber war, precision guided missiles, technological advancements, and computer network attacks provides an opportunity for the United States to conduct a major conflict with an assumed minimization of casualties unlike the Gulf War where casualty estimates were high. The Army National Guard, now a vital ingredient of the National Military Strategy, must learn to fight in a technology-based world. Given the limited training time available and the fact that mission readiness is already a concern, Army National Guard strategic leaders must now, more than ever, establish a basis for successful AC/RC integration. This paper examines the challenges introduced in information warfare and how leaders within the Army National Guard might respond.

As a result of the study, a table for Army National Guard leaders to consider is proposed and discussed. The table addresses issues, concerns, and strategies at the three levels of war: tactical, operational, and strategic. Although several factors impact Guard readiness, this study emphasizes certain factors and provides a basis for Guard leaders when preparing or assessing information warfare capabilities.

Finally, challenges are introduced and discussed. It is imperative that the Guard leadership, leaders of our nation's strategic reserve, ensures a competent and capable 21st Century fighting force. Following the proposed table and addressing the challenges are just two options available to the leadership.

TABLE OF CONTENTS

LIST OF TABLES

Information Warfare and Army Guard Readiness

Even with the longstanding studies of revolutions in military affairs, the decade of the 1990's introduced a new dilemma to military leaders. This dilemma, the introduction of *rapidly advancing* technology into conventional warfare, is not only problematic to the active forces but possibly even more so to the reserve forces. With increased emphasis on force readiness following the United States' victory in the cold war, Army National Guard leaders, already saddled with funding, force structure, training, and end-strength issues, must now examine the impact of operations within the complex and expanding arenas of the newest revolution in military affairs: information and technology.

While information operations have always been a part of warfare, the technologies that implement information operations have never reached this level of efficiency. Digital processing, wireless transmissions, space operations, precision targeting, and all of the connotations accompanying these technologies possibly impact every Army functional area. With advancements continuing, the Army National Guard, established in prestige and honored in its war fighting heritage, must find a way to equip, train, and deploy soldiers capable of effectively using current technologies and capable of operating on a battlefield behest with informational bombardment.

Rationale for the Study

National military strategy dictates that U.S. armed forces should be capable of fighting two nearly simultaneous Major Theatre War (MTW) conflicts and one Small-Scale Contingency (SSC) conflict. Following the draw down of the 1990's, reserve components will play a key role in future military operations. The draw down may not be over. Hart (1998) concluded that technological advancements may result in smaller forces. Active units will be lighter, more agile, more mobile, and highly technical. He further concluded that the majority of the combat focus will shift to the guard and reserves. As a consequence, Hart indicated a need to reshape force structure and modify doctrine resulting in a better-equipped, better-trained guard.

On the other hand, the increased complexity and efficiency may result in troops and commanders being overwhelmed by "information overload". Guard soldiers will have to be highly proficient and competent perhaps indicating a need for better recruits. Information warfare is more than just technology. It is the ability to use information to your advantage on the battlefield. Thus, commanders will also have to become more proficient and competent in such areas as information management and information filtering.

Purpose and Limitations of the Study

The purpose of this study was to identify factors within information warfare that impact guard readiness and to develop a method or methods to minimize the impact. Although the Army National Guard and the Army Reserves share many characteristics, this study concentrated on the guard aspects. Also, this study did not consider Air National Guard properties although they too might share some characteristics.

Scope

This study considered the following two definitions from Joint Publication 3-13 (1998) as a basis. Information operations are the actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks. Information warfare is the information operations conducted during times of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. However, information warfare and information operations are used interchangeably throughout the document based on the following assumptions:

1. Given their shared tenets, information warfare, information operations, cyberspace, information-based warfare, and information-in-war issues impact guard readiness equally.
2. Technology, digitization, and information technology concerns encompass common principles regarding guard readiness.
3. For the purposes of this study, tactical units are traditionally defined maneuver units or combat units. Operational units are theatre-level support units.

Readiness Concerns of Guard Units

Readiness for Army National Guard units is best broken down into two phases: pre-mobilization and post-mobilization. Understanding that mission performance is an important measurement of readiness, effective training becomes a critical tool for "readying" a unit. Pre-mobilization training is often constrained by time and resources. Other constraints include administrative requirements, distance to training sites, and lack of effective exercises. Lippiatt, Crowley, and Solinger (1998) introduced a training model for post-mobilization requirements for combat units. While the model does consider staff training issues that may include information warfare, the model does not directly address it. Regardless of the phase, advanced technologies and the dynamics introduced by the advancements, especially information technology, were not adequately addressed with respect to Army National Guard units.

The Federation of American Scientists (1999) discussed concerns regarding the training proficiencies and mobilization requirements of the enhanced brigades citing an expected postmobilization period of 68 to 154 days and no short-term solution in sight. Lippiatt, Crowley, and Solinger (1998) studied the postmobilization readiness requirements for ARNG integrated heavy divisions. They, too, listed many concerns. Among these were the training resources required for the divisions both post and premobilization, the number of days to ready a division (130 days plus), and the support requirements for training (e.g. instructors, equipment). Thus, both studies addressed the difficulty in preparing Army National Guard units for deployment. But, neither study directly nor even indirectly addressed information warfare and the added complexities that it brings.

The National Guard and Strategic Power

Concerns regarding the United States' ability to employ military power to exert influence in situations involving national interests involve not only the Army National Guard's role in military affairs but also the role of the military in general in such areas as peacekeeping, humanitarianism, and United Nations' operations. Within the framework of power, the Army National Guard constitutes a significant portion of the military piece of the pie. With the advent of "the Total Army' and subsequent "the Army", not only is the percentage of guardsmen a critical aspect, but, also mission apportionment, mobility requirements, employer concerns, and family separations all surface as potential roadblocks to an effective implementation of military power.

Guard units are officially included in the power formula through their inclusion in the National Military Strategy (1997). Directly, reserve components are identified as essential participants in the full range of military operations and as an important indicator of the commitment of the national will. Guardsmen, now integrated into war plans, provide critical skills. Guardsmen also furnish the National Command Authority with a strategic hedge against uncertainty.

Indirectly, Army National Guard units face the same issues as their active component counterparts. The National Military Strategy (1997) also addressed, among other critical militaristic skills, readiness, information operations, asymmetric challenges, and peacetime operations. The Guard, its leaders, soldiers, and plans must address not only these critical areas but also the added onus of being an integral proportion of the main thesis of the National Military Strategy: shape, respond, and prepare.

Introducing Information Warfare into the Mix

Information warfare can best be analyzed within the realm of United States Army War College Course 2 Model (2000) titled "War, National Policy & Strategy". According to the model, wars are fought at the strategic, operational, and tactical level. Information is recognized as an instrument of power by the model. There are numerous possible consequences of overtly introducing information technology and digitization into warfare. For example, Hart (1998) discussed the relevance of platform compatibility among services and units. He also recognized the possibility of advanced technology reducing mass and numbers. Molander, Riddile, and Wilson (1996) developed the concept of strategic information warfare defining it as the utilization of cyberspace to affect strategic military operations and inflict damage on national information infrastrutcures.

Information Power and Strategy

Arquilla and Ronfeldt (1996) discussed information as an instrument of power. They identified three magnitudes of power: material, organizational, and immaterial in nature. Power defined in terms of resources provides capabilities to coerce or otherwise control or influence an actor. In this realm, information is often regarded as simply a raw material or, specifically, a message. Power as organization was defined in terms of how an actor or system organized the resources and capabilities at its disposal mostly a function of the design, implementation, and performance of a resource base. In this realm, information is mostly regarded as a system capable of sending and receiving messages. The third magnitude, power as immaterial, was less precise but centered on the view that power is metaphysical and more abstract. In this abstract realm, theorists regard information as an embedded physical property of all objects that exhibit organization and structure.

Joint Vision 2010 (1997) suggested information dominance as a military goal. Other power bases recognized by Joint Vision 2010 were economics, politics, and military. Arquilla and Ronfeldt (1996) identified wisdom as the highest level of information and knowledge as the next highest level. They called for continuing research regarding the implication of informational power as applied to military situations. In conclusion, information is commonly recognized as a component of national power and an important player in the military environment.

The Strategic Level and Information Warfare

Wilde (1998) stated that the strategic objective of information warfare was to affect adversarial decision-makers to the degree that they cease any actions threatening the United States' national security interests. He recognized that the United States was facing an increased critical dependence on information and information systems. Peartree, Allard, and O'Berry (1997) stated that information systems were integrated in to the four pillars of Joint Vision 2010: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. They felt that the targeting or protection of homeland assets such as the critical national infrastructure was a strategic dimension of information warfare. Gumpert, Kugler, and Libicki (1999) discussed a "system of systems" that included sensors, networks, databases and weapons.

The Operational Level and Information Warfare

Peartree, Allard, and O'Berry (1997) defined operational warfare as targeting or protecting information assets at the level of campaigns. This is consistent with Builder's (1997) definition of operational warfare as providing the means for strategic warfare in that both address the campaign level. Wilde (1998) defined information operations as exploiting the vulnerabilities and opportunities of information and information systems.

Wilde further noted that rapid advances in information technology substantially increased the amount and availability of information and the complexity of information systems that support military operations. He concluded that information superiority translates to better situational awareness resulting in faster and more effective decisions.

Shelton (1998) felt that information technology could provide battlefield commanders with a complete picture of enemy threats and opportunities. He surmised that we could put many weapons on target in a matter of minutes or even seconds. In this context, information is best viewed as an available course of action.

The Tactical Level and Information Warfare

Understanding the significance of the Guard's role in the operational, strategic, and national power realms and accepting the unavoidable proliferation of information operations and technology, Guard leaders face the challenge now of making units mission capable in an advanced technological environment. While currently residing mainly in communications units, information technology will soon impact all units and branches. Tactical and technical proficiency must almost assuredly, within the context of readiness, address information operations in some manner and demand a minimum level of competence or comfort from every Guard soldier. Viewed historically as a technical skill due to the high technology communications and computer equipment, information operations, possibly attributable to ease of use, is rapidly evolving into an assumed tactical skill.

Tactical impacts regarding information was also addressed in the literature. Peartree, Allard, and O'Berry (1997) used the word information when defining warfare. They defined it as as the ability to disrupt, disable, deny or exploit enemy battlespace information and to protect one's own. The 1998 draft of FM 100-6 stated that the most probable means for informational tactical operations involve direct and indirect fires. Other tactical tasks or considerations mentioned in FM 100-6 included mission analyses, lack of assessment of effectiveness of offensive information attacks, OPSEC, physical security, intelligence, surveillance, and reconnaissance. The major underlying concerns at the tactical level are the lack of assessment capabilities and the volume of information flow.

Concentrations within Information Warfare

To better identify tenets within information warfare, seven concentrations were chosen to use as a guide to assess the completeness of the existing framework: attainments (end), organization type (way), platform concerns (way), characteristics (way), tasks (mean), proficiencies (mean) and connectives (mean). This introduction of concentrations provides Army National Guard leaders at all levels a system for preparing Army National Guard units to fight efficiently and effectively in information warfare.

Attainments

Attainment can be viewed as the achievement of a specific goal. In higher education, Pascarella and Terenzini (1991) associated attainment, the acquirement of a bachelors degree, with factors such as student commitment, institutional mission, institutional type, and institutional racial composition impacting the attainment or non-attainment of the degree. Relating this to information warfare, the mission of the unit, the type of unit, and unit composition all might impact an expected attainment or outcome of successful performance in an information warfare scenario.

Arquilla and Ronfeldt (1996) identified wisdom and knowledge as expected outcomes of informational power. FM 100-6 (1998, draft) discussed public support, information superiority, information management, and credibility as conceivable outcomes. Attainments at the unit level could be soldier competence and mission capability.

Organization Type

Whether a maneuver unit or a theatre-level unit, information technology will have an impact. However, the impact will vary greatly dependent upon the mission and unit capability. Thus, organizational make-up becomes a planning factor. Although the literature did not specifically address organization in the realm of ends-ways-means, four organization types correlate to informational power and the three levels of war. The four associated types are policy-making, support, separate, and integrated.

Platform Concerns

Another planning consideration for acquiring our desired attainments deals with platform concerns. Recognizing and interpreting platform issues and implementations becomes substantial on the pathway to success. Suggested platform concerns based on my experiences with information systems are supremacy, infrastructure design, reliability, interoperability, redundancy, and familiarity.

Characteristics

Using Arquilla and Ronfeldt (1996) as a guide, characteristics were viewed as an embedded property of raw information. Information must be useful in many forms. Understanding these uses and the levels that they fall under provides Army National Guard leaders a powerful strategic and operational advantage. FM 100-6 (1998, Draft) identified five characteristics of information:

Accuracy: The extent to which information conveys the true situation.

Timeliness: The extent to which information is available in time to make decisions.

Usability: The extent to which information conforms to common, easily understood formats and displays.

Completeness: The extent to which the information contains all of its parts.

Precision: The extent to which information has the required level of detail.

A sixth characteristic, *coherence*, must be considered. While the FM 100-6 definitions address truth, availability, understandability, totality, and detail, they do not address a required, inherent characteristic of logical connectivity at the highest level. Coherence is the extent to which the datum fits into the overall picture.

Tasks

There are numerous tasks associated with information warfare and information operations. However, certain tasks are essential to operational effectiveness. Mastering appropriate information operations tasks yields Guard leaders another resource for ensuring success. Offensive tasks identified in FM 100-6 were operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare, physical destruction, and special information operations, and could include computer network attack. Defensive tasks identified were information assurance, physical security, operations security, counter-deception, counter-propaganda, counterintelligence, electronic warfare, and special information operations. Additional tasks required above the maneuver level might be guidance, infrastructure security, research, and joint awareness. Additional tasks required at the maneuver level include intelligence, surveillance, and reconnaissance. Some tasks shared common traits and/or appeared repetitive and were absorbed into similar tasks for this study resulting in operations security, physical security, deception, electronic warfare, intelligence, surveillance, reconnaissance, PSYOP, infrastructure security, network attack, guidance, joint awareness, and research.

Proficiencies

Certain skills or talents are necessary in information technology fields. Interjecting the complexity of warfare, these skills or talents become critical. Existence of these talents becomes a crucial resource for Guard leaders. Emphasizing theoretical understanding, automation conceptuality, risk assessment, battlespace awareness, and unit training effectiveness at the appropriate level of warfare or within the realm of national power enhances success.

Connectives

Connectives are associated concerns of information warfare and become a means in that they are resources or talents for effectiveness. Suggested connectives are entropy recognition, complexity management, funding, cyberspace awareness, system analysis techniques, and aptitude.

Synopsis of the Concerns

Readiness of Army National Guard units remains an issue. Information warfare heightens readiness concerns. Army National Guard strategic leaders are fast approaching a critical moment. Can Guard units, currently equipped with 20th century equipment and training methods participate effectively on the 21st century battlefield. Several factors complicate the matter including size, mission, and expected area of operations. Complicating the matter even more is the on-rushing tide of information technology. Discontinuity perpetuates the literature. By reducing redundancy and eliminating ambiguity, Guard leaders can better prepare a very crucial strategic asset in the National Military Strategy, the Army National Guard. The need exists for a method or model that provides an adequate basis to unite these two areas of concern: Guard readiness and information warfare.

Proposed Categorization

Given the complex and varied applications and definitions of information technology in warfare, guidelines are needed for Army National Guard leaders. Seven concentrations were constructed to better organize existing findings, to better identify common tenets among the works, to reduce redundancy, and to simplify the maze of definitions. These categories were attainments, organization type, platform concerns, characteristics, tasks, proficiencies, and connectives. Each level of warfare, tactical, operational, and strategic, was addressed within the context of Chilcoat's (1995) construct of ends, ways, and means. Specifically, the aim was to provide a basis to the information warfare literature within the context of power and the three levels of warfare resulting in a method or strategy for Guard leaders. Table 1 depicts the recommended categorizations for addressing Guard readiness within the realm of information warfare.

		Information Warfare Level			
		Tactical	Operational	Strategic	Power
Concentrations	Attainment (ends)	Soldier competence, Mission capability	Superiority, Management	Public support, Credibility	Wisdom, Knowledge
	Organization (ways)	Integrated	Support	Separate	Policy
	Platform Concerns (ways)	Familiarity	Interoperability, Redundancy	Infrastructure design, Reliability	Supremacy
	Characteristics (ways)	Usability, Timeliness, Precision	Accuracy	Completeness,	Coherence
	Tasks (means)	OPSEC, Physical security	PSYOP, Deception, EW, Intelligence, Surveillance, Recon	Infrastructure security, Network attack	Guidance, Joint awareness, Research
	Proficiency (means)	Unit training effectiveness	Risk assessment, Battlespace awareness	Automation conceptuality	Theoretical understanding
	Connectives (means)	Aptitude	Systems analysis techniques	Funding, Cyberspace awareness	Entropy recognition, Complexity management

Table 1. Information Warfare Guidance.

Impact of the Groupings

Tactical Integration

In the tactical environment, soldiers are expected to take the fight to the enemy through all means possible. Readiness for Guard units include the same concerns for active units plus the additional concern of limited training time. For Guard soldiers to fight effectively in the information tactical warfare arena, effective schemes and/or methods addressing the end-state for tactical readiness, namely soldier competence, and mission capability are needed. Employing Table 1, Guard commanders, regardless of the type of unit, can better ensure information readiness by finding the correct column and working their way up through the table using the following discussion as guidelines.

Accepting that ways are methods for using resources to reach our attainment, the major information warfare resource available to the tactical commander is the technical aptitude of his/her soldiers. Technology skills are fast becoming a necessary common soldier skill. Zeroing in on aptitude, commanders can employ several plans resulting in soldier competence and mission capability. Gagne (1985) suggested that, regardless of the subject complexity, students fall into one of several different levels of competence necessitating different approaches to training based on the respective level. Thus, even soldiers with a generally low aptitude for a particular subject may obtain competence through effective training. Unit training effectiveness is the key to success. Guard commanders should consider:

1. Recognizing the importance of tactical communications equipment and emphasize communications training.
2. Identifying a common set of basic skills such as email, word processing, file saving, data backup, file transfer, and software installation.
3. Identifying key information-based positions within the unit.
4. Identifying additional skills for these key positions such as hardware maintenance, software maintenance, data recovery, networking, connectivity, and soldering.
5. Identifying unit personnel with a high aptitude for technology.
6. Integrating the necessary training into the yearly training plan driven by the aptitude-level of the soldiers. Means available, among others, include State ADP organizations, local colleges, local vocational-technical schools, and high-aptitude soldiers within the unit.
7. Providing refresher training and/or testing for all unit personnel.
8. Continued assessment of the unit's information technology skills.

A key consideration for producing a mission capable unit is the tasks required in the battlefield. With limited training time, Guard commanders must choose which tasks are appropriate for their unit given their mission. Of the tasks identified by FM 100-6 (1998 draft), two are critical to all units, regardless of their information orientation. Operations security and physical security are components of survivability. Acknowledging this, Guard commanders must:

1. Ensure effective communications security procedures are addressed in the yearly training plan.
2. Ensure that soldiers follow adequate ADP security practices such as shielding monitors, using secure lines, using accredited computers, and completely erasing files.
3. Incorporate ADP physical security concerns into the unit physical security plan.
4. Incorporate ADP concerns into the field standard operating procedures.

Continuing up the table, the three critical characteristics of information at the tactical level are usability, precision, and timeliness. Emphasizing the ability to determine the preciseness of received information provides commanders increased tactical proficiency though better awareness. Conversely, units possess an inherent responsibility regarding the usability of disseminated information. Timeliness is particularly an issue at the tactical level. Specifically, Guard commanders should:

1. Ensure that information requests are answered in an expedient manner.
2. Provide crosschecks and appropriate approval level for dispatched messages.
3. Provide sound procedures for processing information within the unit TOC.
4. Follow proven methods for communications security.
5. Ensure soldier familiarity with information warfare issues and procedures.

Concerns with platform familiarity transcend several military weapons systems. This critical notion, the notion of competence with a particular technology, increases in scope in the information technology field. Continued increases in processor speed, random access memory, fixed storage space, operating system functionality, and peripheral device availability lead to a wide variety of ever-changing platforms. Impacts may include a training program centered around a platform rendered obsolete or ineffective at the onset of hostilities. Guard commanders can:

1. Emphasize basic communications skills.
2. Emphasize basic computer skills.
3. Scan the environment for expected changes to computers in general.
4. Scan the environment for expected changes to unit computer and communications equipment.
5. Create and maintain a feasible migration plan based on current unit technologies and possible changes.

Maneuver unit commanders and support units in the main battle area must find effective ways to incorporate information technology. Most probably, information systems support will be integrated within the unit through cross training vice dedicated positional support. Accepting this fate, Guard commanders may ensure adequate supports exists by:

1. Coordinating with the appropriate external military support units.
2. Identifying civilian contractors and the means for employment.
3. Preparing contingency plans for loss or failure of ADP equipment.
4. And, as always, stressing basic computer and communications skills.

Soldiers with a high aptitude for information technology become an asset in the training program. By employing these methods, based on assessed soldier aptitude and resulting in soldier competency, tactical commanders lay the groundwork for success on the tactical information battlefield.

Operational Integration

Understanding that the complexity in information warfare increases with each subsequent level of warfare, commanders face similar concerns at the operational level as at the tactical level but with increased technological conceptuality. For instance, many maneuver units operate at the operational level. Each commander must review his capabilities and his real world mission to determine which integration is best suited for his/her unit. Most likely, at the operational level, communications, automation, and intelligence will merge more directly into unit functions. For combat units operating in the operational environment, the previous section will still most likely apply. For specialty units such as echelon above corps units, area support groups, and others, the following may apply. Table 1 again provides a guideline for commanders.

One major information warfare resource available to the commander whose unit is fighting in the operational environment is the capability to perform systems analysis functions. Analytical capacity provides methods for performance analysis, hardware configuration, software troubleshooting, and user interaction. Using systems analysis, Guard units may improve their chances for successful mission integration. Also, communication protocols necessitate information not only connecting to the tactical operations but also to the strategic level serving and, in essence, serving as a bridge between the two. Guard commanders functioning on the operational battlefield should consider:

1. Placing a heightened emphasis on analytical skills.
2. Encouraging knowledge of and/or familiarity with communications and signals equipment.
3. Encouraging knowledge of and/or familiarity with intelligence equipment and doctrine.
4. Ensuring training in security and operations security requirements.
5. Continued assessment of unit's information technology skills.
6. Encouraging knowledge of and or familiarity with connectivity hardware and protocols.

Two things are critical for survivability and success in the operational environment: risk assessment and battlespace awareness. Constant evaluation of the enemy and friendly situation become particularly significant due to the importance of upward and downward communication. Soldiers in rear area units must know what risks exist to the communications infrastructure and what the battlespace looks like to correctly parlay true information to tactical units. Suggestions include:

1. Developing risk assessment procedures that directly address information operations and warfare.
2. Incorporating procedures ensuring constant assessment of the battlespace and appropriate dissemination of the status.

Table 1 identifies six key tasks from FM 100-6 (1998 draft) that are critical at the operational level. These six tasks are deception, electronic warfare (EW), intelligence, surveillance, and reconnaissance. The FM states that at the operational level of war deception may be the significant offensive information operations measure. Electronic warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy. Guard leaders must understand the importance of PSYOPs as an offensive weapon. Whether leaflets, loud speakers, or mass e-mailings, operational level Guard units must incorporate PSYOPs training into their training plans. One must never underestimate the criticality of accurate and timely intelligence especially in information warfare. If intelligence involves the collection, analysis, and dissemination of enemy information, then both offensive and defensive operational campaigns rely heavily on competent intelligence systems. Surveillance and reconnaissance are often viewed as subsets of the intelligence system.

Accuracy is the key informational characteristic at the operational level. The operational level provides the first key chance to filter information, organize it, and disseminate it in a systematic manner. By systemizing the collection process, units can employ better methods for verifying the validity of the data. Guard commanders can use training exercises to teach effective filtering, organizing, and disseminating of information.

Because of the need to connect the tactical level to the strategic level, major platform concerns at the operational level center around interoperability. Whether addressing automation or communications equipment, the methods currently used to field systems places Guard units at a distinct disadvantage. Guard units are often far behind their active army counterparts. In addition to hardware compatibility, automation introduces software, peripheral, and operating system compatibility issues. Redundancy, the ability to continue operations despite a failure usually through duplicate, stand-by equipment, is probably a luxury in the military with its expected level of attrition. However, redundancy must be addressed. Additionally, commanders should consider:

1. Scanning the environment for expected changes to computers in general.
2. Identifying units, either active or reserve, in your training area of operations that possesses equipment similar to what you expect to use in an information warfare campaign and arrange a training agreement.
3. Scanning the environment for expected changes to unit computer and communications equipment.
4. Creating and maintaining a feasible migration plan based on current unit technologies and possible changes.

One way to distinguish between information operations at the operational level versus the tactical level of warfare is support response time. Knowing that a dedicated support system probably exists and how to access it is critical for commanders. Additionally, commanders, knowing that their mission, MTOE, or scenario implies rapid information operations support, can supplement or augment their mission essential task list as appropriate. EAC and other specialty units can also modify their mission essential tasks list accordingly. Ultimately, information superiority and information management are the goals attained at the operational level.

Strategic Integration

The Army National Guard faces many obstacles in meeting the information challenge. Because of its orientation, strategic plans involving the Army National Guard might require negotiation among 54 adjutant generals, National Guard Bureau officials, Active Army officials, Army Reserve officials, and any other number of possible participants. Multi-composition units, units shared among states, and equipment fielding practices also add to the mix.

Guard leaders must seek an additional level of appropriate funding to ensure that every state and every unit is properly equipped and properly prepared. With the procurements comes the responsibility of ensuring that appropriate personnel are aware of issues and advancements in cyberspace. Whether GPS, Combat Identification (CID), Battlefield Awareness and Data Dissemination (BADD), or Dynamic Database Program (DDP), leadership awareness becomes a critical factor. This knowledge base needs to escape the confines of the full-time force and make its way to every battalion in every state.

Additionally, strategic Army National Guard leaders must develop a certain level of automation conceptuality. At the National Guard Bureau, plans are underway to ensure that State

Area Commands are sufficiently capable to process diverse mission requests, to establish a knowledge infrastructure, and to install a data transport system. Division, brigade, and battalion commanders and staffs need inclusion in the process and ultimately the system. Capabilities exist that could allow key Army National Guard M-day leaders access to unclassified systems from their homes.

Strategic tasks for Guard leaders consist of infrastructure security and the ability to prevent of initiate computer network attack. The knowledge infrastructure will include every STARC. Thus, every STARC may be subject to some type of asymmetric infrastructure or computer network attack. Protecting physical lines of communications, whether homeland or theatre, is crucial.

Completeness is the extent to which information contains all of its parts. At the strategic level, incomplete information should not be discarded. Rather, it should be saved and constantly reexamined. The goal at the strategic level is to form a total information picture of the situation. Complete information fulfills that goal.

Reliability affords many desirable traits such as operability, weapons precision, systems confidence, and checks and balances. Proper infrastructure design sets the foundation for existing and planned systems at the national level. To ensure integration and interoperability, Army National Guard leaders at the strategic level should recognize the importance, the intensity, and the volume of work involved in the management of information systems. At this level, to fully support inclusion in the national infrastructure and to ensure complete integration, the Army National Guard should turn to external sources for appropriate support knowledge. One possible external source is the active Army. Another is outsourcing.

Finally, the Army National Guard has long recognized the need for public support and has been often employed as a means to gain public backing of a conflict or operation. Credibility is critical to a successful information operations organization. The Army National Guard must play its part in establishing credibility prior to and during any conflict involving information warfare. Specifically, to ensure proper inclusion, Guard leaders can pursue:

1. Elevation of the Chief, National Guard Bureau, to a 4-star, and include on the Joint Chiefs of Staff.
2. Creation of an Information Warfare cell within Joint Forces Command and include a Guard General Officer.
3. Encouraging Congress to change existing policies regarding the equipping of the Guard.
4. Developing appropriate procedures and guidelines for training Guard units to fight at either the tactical or operational level as necessary using Table 1 as a guide.

5. Acquiring additional funding from befitting sources for the purposes of information warfare training.

Challenges to the Strategic Leaders of the Army National Guard

Within the context of readiness and integration, the Army National Guard still faces many challenges. One challenge facing Army National Guard Strategists is the role the Guard plays in establishing or generating public support for conflict involvement. Public affairs, a key function in information warfare, becomes critical when the United States elects to send troops to engagements not directly or apparently not directly applicable to the country's vital interests. If Guardsmen, men and women from local communities holding down jobs such as principal, policeman, teacher, or sales clerk, are sent, then community reaction is swifter and more stringent. Once called, it becomes incumbent upon Guard leaders to foster a sense of local support from families, communities, and employers perhaps through an energetic public relations campaign devised specifically for this purpose.

Another challenge is the rapid advancement of technology. Guard Vision 2010 recognized the key role that technology, automation, and infrastructure play in today's fighting force. Though considered the strategic reserve, second and third order effects from being ill-equipped or ill-trained on state-of-the-art equipment must be considered. These effects, regardless of CONUS or OCONUS, might include vulnerability to Computer Network Attack, the inability to communicate on the battlefield, the inability to assimilate properly into the intelligence arena, and the inability to successfully manage the potential overload of information. Guard Vision 2010 addresses many of these concerns. Guard leaders, given the ever-changing technological world, must continually update plans and address concerns as changes occur or threaten to occur.

Another key information warfare concern for Army National Guard leaders is the possible and significant shift from a military posture of victory through firepower to one of victory through covertness. With a significant portion of the Army National Guard consisting of combat arms units and with the current Chief of Staff of the Army insisting on changing to a lighter yet lethal force structure, Guard leaders may find themselves with 21st century units ready, trained, and equipped to fight a 20th century war. One way to address this problem is insistence on changing the current funding and equipping paradigm. Rather than continue the methods of equipping the active components first and passing the older equipment down to the Guard, the Army would do better to replace its "first to fight" method with a "first to mobilize" equipping paradigm. By insisting on this strategy, Guard leaders heighten training and readiness and increase the likelihood of Guard soldiers performing effectively on the battlefield by breaking down complexity barriers often associated with technologically based equipment.

However, the greatest challenge is most probably not Guard unique. That challenge, recruiting soldiers intelligent enough, competent enough, and swift enough to grasp information technology concepts and implementations, faces all sectors of the armed forces. But, the challenge is magnified in the Army National Guard due to the limited training time. Guard leaders must insist on top-notch recruits to fill the ranks. One possible answer is to eliminate the current recruiting competition between the Active Army and the Army National Guard and establishing a cooperative or even consolidated recruiting element.

Summary and Recommendations

When employed correctly, the Army National Guard becomes an integral part of national power. If integrated and aligned properly, Army Guard units and leaders better understand and subsequently help ensure that the nation achieves this power. Given the criticality of the Army National Guard to the National Military Strategy, it is no longer a plausible option to exclude this part-time force from the workings of the systems used to support the full-time force. The Army National Guard must participate at every level, in every arena, and on every platform. Areas traditionally non-Guard inclusive, whether by design or by accident, such as the Joint Chiefs of Staff, the POM process, and TRADOC, face compelling reasons to broaden their scope and support the concept of "the Army".

Information warfare introduces many new dilemmas. However, the potentials and possibilities greatly outweigh the concerns associated with these enigmas. It is compelling upon the Army National Guard's strategic leaders to ensure that Guard units are properly equipped, properly manned, and properly trained to fight the next war. The changes required are strategic in nature and must start at the top.

Word Count:

5964

Bibliography

Arquilla, J. and Ronfeldt, D. (1996). Information, Power, and Grand Strategy: In Athena's Camp-Section I. In The Information Revolution and National Strategy: Dimensions and Directions. Edited by Stuart J. D. Schwartzstein, Washington D.C.: CSIS.

Builder, C.H. (1997). Keeping the Strategic Flame. Joint Force Quarterly. Winter, 1996-1997.

Chilcoat, R.A. (1995). Strategic Art: The New Discipline for 21st Century Leaders. U.S. Army War College, Strategic Study Institute Publication, 10 October 1995.

Federation of American Scientists (1999). Army National Guard: Combat Brigades Ability to Be Ready for War in 90 Days Is Uncertain. 6 June 1999. Available from http://www.fas.org/man/gao/ns95091.htm. Internet accessed 11 November 1999.

Gagne, R. (1985). The Conditions of Learning (4th ed.). New York: Holt, Rinehart & Winston .

Gumpert, D.C.; Kugler, R.L., Libiki, M.C. (1999). Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs. National Defense Univerity.

Hart, G. (1998). The MINUTEMAN, Restoring an Army of the People. The Free Press, a Division of Simon & Schuster Inc. New York, NY.

Lippiat, T.C.; Crowley, J.C.; Solinger, J.M. (1998). Time and Resources Required for Postmobilization Training of AC/ARNG Integrated Heavy Divisions. RAND.

Molander, R.C.; Riddile, A.S.; Wilson, P.A. (1996). Strategic Information Warfare: A New Face of War. RAND.

Pascarella, E.T. and Terenzini, P.T. (1991). How Colleges Affects Student. Jossey-Bass Publishers, San Francisco, CA.

Peartree, C.E.; Allard, C.K.; O'Berry, C. (1997). Information Superiority. In Air and Space Power in the New Millennium. Edited by Daniel Goure' and Christopher M. Szara. CSIS.

Shelton, H.H. (1998). A Word from the New Chairman. Joint Forces Quarterly. No. 17.

U.S. Army War College. Core Curriculum Course 2: War, National Policy & Strategy. Directive, Department of National Security and Strategy. U.S. Army War College. Carlisle Barracks, PA 17013-5050. Academic Year 2000.

U.S. Department of the Army. Information Operations. FM 100-6. Washington D.C.: U.S. Department of the Army, August 1996.

U.S. Department of the Army. Information Operations. FM 100-6 (Draft). Washington D.C.: U.S. Department of the Army, 1998.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: U.S. Joint Chiefs of Staff, 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Vision 2010. Washington D.C.: U.S. Joint Chiefs of Staff, 1997.

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America. Joint Publication 3-13. Washington D.C.: U.S. Joint Chiefs of Staff, 1997.

Wilde, A. (1998). Update: Information Operations. A Common PERSPECTIVE. Volume 6, No. 2.